Sl

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/704,790	11/03/2000	Walter Mason Stewart	109993.00103	7495

27557 7590 05/21/2003

BLANK ROME COMISKY & MCCAULEY, LLP
900 17TH STREET, N.W., SUITE 1000
WASHINGTON, DC 20006

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	**PAPER NUMBER**
2131	12

DATE MAILED: 05/21/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Sl

Office Action Summary	**Application No.** 09/704,790	**Applicant(s)** STEWART ET AL.	
	Examiner Paula W Klimach	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 March 2003* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☒ Interview Summary (PTO-413) Paper No(s). *12* .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

1. **Claims 1-41** are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The method for choosing the conversion process depending on the type of email is not discloses in the specification. Claim 1, 16, and 31 recites that an executable format will be converted to a non-executable format by a plurality of conversion processes selected in accordance with a type of e-mail. On page 5 of his response the applicant directs attention to page 5 line 14 to page 7 line 18 of the specification as support for the amendment.

However, the description in the specification does not explain the conversion process that depends on the type of email for converting from executable format to non-executable format. The specification gives that example of a PDF file as one type non-executable format, but does not indicate the different types of format that the different types of email can be converted to.

New matter as specified above must be cancelled from application. Claims that are not specifically addressed are rejected by virtue of their dependency.

2. **Claims 1-41** are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to enable one skilled in the

art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification describes converting executable format to non-executable format and gives the example of PDF file as non-executable format. However, claim 1, 16, and 31 states that to convert the email from executable to non-executable a plurality of conversion processes selected, depending on the type of email, is provided. Since only one conversion was described in the specification, finding other processes to convert the executable format to non-executable format would required experimentation with different processes. The experimentation would be required to find other forms of non-executable files to convert the executable file to, apart from the PDF file mentioned, which has only one format.

Claims that are not specifically addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 102

> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

3. **Claims 1, 16, and 31** are rejected under 35 U.S.C. 102(e) as being anticipated by Kellum (6, 487, 664) and the Microsoft Computer Dictionary.

Kellum describes a method for protecting a network, claim 1 lines 1-3. The Kellum system protects the network from hostile data (viruses), contained in the information exchange between a protected network and the external information source, claim 1 lines 1-11. An email message is a form of information, in the form of text messages and computer files, which is exchanged over a computer network, Microsoft Computer Dictionary page 173. The Kellum system receives the messages through an intermediate computer hardware device IDS 12, fig. 2, claim 1 lines 8 and 9. The intermediate domain screen IDS serves as a gatekeeper server. Kellum system also converts the e-mail message from an executable format to a non-executable format, claim 1 lines 14-18. The Kellum system chooses from a plurality of conversion processes, column 9 lines 56-60. Furthermore, the Kellum system also maintains the appearance, human readability and semantic content of the email, by creating a second format that contains the information from the first format, claim 1 lines 16-18. Finally the Kellum system sends the email to the recipient, claim 1 lines 19-22.

Furthermore, Kellum disclose a system that chooses from a plurality of processes selected in accordance with the type of email, column 11 lines 11-25. In this section of the specification Kellum indicates that the type of transformation of the first format to the second format depends on the format of the incoming signal.

Claim Rejections - 35 USC § 103

4. **Claims 2 and 17** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum as applied to claims 1 and 16 respectively above, and further in view of Cornetto et al.

Kellum does not describe executable code embedded email as files that can contain viruses.

Cornetto teaches of HTML formatted email, which acts like a browser, page 1 paragraph 4 and 5.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to receive the email Kellum's virus elimination system, run the HTML formatted email, the executables within the email as described by Cornetto (page 2 paragraph 1), in the intermediate domain device before, it is sent to another user. One of ordinary skill in the art would have been motivated to do this because embedded executables run locally and if they contain malicious scripts they could create disruptive virus behavior, Cornetto page 2 paragraph 1.

5. **Claims 3 and 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum and Cornetto, as applied to claim 2, and 17 respectively above, and further in view of Allen (5940614) and Brown.

Allen discloses a system that can deactivate and reactivate hyperlinks to provide a hypertext control method and apparatus in which different hypertext information or different target modules are displayed based upon a user class or authority, column 2 lines 2-6.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to receive in the intermediate domain device as described by Kellum, and deactivate hyperlinks as in Allen. One of ordinary skill in the art would have been motivated to do this because clicking on hyperlinks in email can lead to virus infection, Brown paragraph 20.

6. **Claims 4, 5, 20 and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown in view of Kellum.

In reference to claim 4 and 19, Brown teaches that executable files attached to e-mail could cause a virus to infect a computer, page 2 paragraph 1.

Brown does not teach of a system to protect the network against the fore mentioned viruses.

Kellum describes a method for protecting a network, claim 1 lines 1-3. The Kellum system protects the network from hostile data (viruses), contained in the information exchange between a protected network and the external information source, claim 1 lines 1-11.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the Kellum network protection system on the email described by Brown. One of ordinary skill in the art would have been motivated to do this because universal protection of information is needed, whereby protection is easily verifiable, cost-effective, and does not require prior knowledge to successfully execute a detection, Kellum column 2 lines 31-35.

In reference to claims 5 and 20, Kellum further teaches of the intermediate domain device being made up of sockets, which connect the IDD to the external system, column 2 lines 46 and 47. These sockets perform the task of the gatekeeper, column 6 lines 40-48. The socket sends these signals to the sacrificial server (the intermediate domain device IDD), Fig. 2. The IDD then converts executable files into non-executable files during the modified read claim 1 lines 14-18.

7. **Claims 6, 7, 21, 22, 32, and 33** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum and Brown as applied to claims 4, 16, and 31 above, and further in view of Schnurrer et al (5,842,002).

In reference to claim 6, 21, and 32, Kellum and Brown do not expressly disclose looking for virus activity.

Schnurer discloses a system that looks for computer virus activity which include changes in the IRQ table, FAT, and files, Fig. 6C.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to look for virus activity in server 20. One of ordinary skill in the art would have been motivated to do this because virus activity indicates the presence of a virus in the network, Schnurer column 7 lines 53-67.

In reference to claim 7, 22, and 33, Kellum discloses a system where in the case of contamination of the IDS from hostile code the IDS can be rebooted safely from a safe copy of the operating system, column 4 lines 39-42.

8. **Claims 8 and 23** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum and Brown as applied to claims 5 and 20 respectively above, and further in view of Swift et al (6,377,691 B1).

Kellum and Brown do not disclose a method wherein communication between the gatekeeper server and the sacrificial server is authenticated using a challenge-and-response technique.

Swift discloses a system that uses a challenge-response authentication technique to authenticate the communication between a client and server, abstract.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a challenge-response authentication technique to authenticate the sacrificial server, 20. One of ordinary skill in the art would have been motivated to do this because the challenge-response authentication technique prevents the replay of messages therefore detecting intruders, Swift column 3 lines 19-21 and column 3 lines 44-46.

9. **Claim 34** is rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum and the Microsoft dictionary as applied to claim 31 above, and further in view of Swift.

Kellum does not disclose a method wherein communication between the gatekeeper server and the sacrificial server is authenticated using a challenge-and-response technique.

Swift discloses a system that uses a challenge-response authentication technique to authenticate the communication between a client and server, abstract.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a challenge-response authentication technique to authenticate the sacrificial server, 20. One of ordinary skill in the art would have been motivated to do this because the challenge-response authentication technique prevents the replay of messages therefore detecting intruders, Swift column 3 lines 19-21 and column 3 lines 44-46.

10. **Claims 9, 24, and 35** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown and Kellum as applied to claims 4, 16, and 31 respectively above, and further in view of Ji et al (5,623,600) and Battersby et al (5,740,370).

Brown and Kellum do not disclose a system that maintains a list of approved attachment types.

Battersby discloses a system that maintains a list of file type identifiers in order to determine whether a file belongs to a certain file subset of files, column 14 lines 18-25.

Ji discloses a system that determines whether the attachment is of a type, which is in the list of approved attachments types (types that do not contain viruses), fig 6B. Ji also sends a virus detection message to the client as a reply, fig 6B.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain a list of approved attachment types in server 20, determine whether the attachment is a type which is in the list described by Battersby with the method described by Ji, and inform the recipient that a message containing a non-approved attachment has been received, as described by Ji. One of ordinary skill in the art would have been motivated to do this because it would not affect the performance of individual computers, Ji column 2 lines 23-30.

11. **Claims 10, 25, and 36** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum and the Microsoft Computer dictionary as applied to claims 1, 16, and 31 respectively above, and further in view of Ji et al (5,623,600) and Jury et al (5,618,054).

Kellum system also converts the e-mail message from an executable format to a non-executable format, claim 1 lines 14-18.

Kellum does not disclose a system that maintains a list of approved executable code.

Jury discloses a process that maintains a list of files retrieved by the user in order to delete the files when the user terminates the Electronic Performance Support System, column 10 lines 17-22.

Ji discloses a system that determines whether the attachment is of a type, which is in the list of approved attachments types (types that do not contain viruses), fig 6B. Ji also sends a virus detection message to the client as a reply, fig 6B. The types of files that are suspected virus carriers are executable code, column 7 lines 33-40.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain a list of approved executable code as described by Jury, determine whether the attachment is executable code in the list of executable code as in Ji, and deactivate the executable code if it is not in the list, as described by Kellum. One of ordinary skill in the art would have been motivated to do this because maintaining a list of files gives the user a choice of files to deactivate, Jury as shown in column 7 lines 32-38.

12. **Claims 11, 12, 13, 26, 27, 28, and 37** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum, Microsoft Computer dictionary, Ji, and Jury as applied to claims 10, 25, and 36 above, and further in view of Corthell (6,192,477 B1), Horwitt, and Rad.

In reference to claim 11, 12, 26, 27, and 28, Kellum system also converts the e-mail message from an executable format to a non-executable format, claim 1 lines 14-18. This would deactivate the executable code.

Kellum, Ji and Jury do not disclose a method for determining whether the executable code has been altered, using an check-summing algorithmic technique.

Corthell discloses a system that uses the checksum algorithm to determine whether a file has been altered, column 8 lines 7-16.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to determine whether the executable code has been altered using the method of Corthell, using an algorithm. Then deactivate the executable code if it has been altered using the method disclosed by Kellum. One of ordinary skill in the art would have been motivated to do this because checksum is a common way to check if files have been altered, Horwitt, abstract.

In reference to claim 13, Kellum system also converts the e-mail message from an executable format to a non-executable format, claim 1 lines 14-18. This would deactivate the executable code.

Kellum, Ji, and Jury do not disclose a method for determining whether the executable code has been altered, using a check-summing algorithmic technique.

Corthell discloses a system that uses the checksum to determine whether a file has been altered, column 8 lines 7-16.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to determine whether the executable code has been altered, using a checksum algorithm as shown in Corthell. Then deactivate the executable code if it has been altered using the method disclosed by Kellum. One of ordinary skill in the art would have been motivated to do this because checksum is a common algorithm of checking the corruption of files, Horwitt, abstract. If the file has been corrupted (altered), it is possible that it contains a virus, Rad, paragraphs 13-16 and 30.

In reference to 37, Kellum system also converts the e-mail message from an executable format to a non-executable format, claim 1 lines 14-18. This would deactivate the executable code.

Kellum, Ji and Jury do not disclose server for determining whether the executable code has been altered, using an check-summing algorithmic technique.

Corthell discloses a system that uses the checksum algorithm to determine whether a file has been altered, column 8 lines 7-16.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to determine whether the executable code has been altered, using a checksum algorithm, as shown by Corthell. Then deactivate the executable code if it has been altered, using the method disclosed by Kellum. One of ordinary skill in the art would have been motivated to do this because checksum is a common algorithm of checking the corruption of files, Horwitt, abstract. If the file has been corrupted (altered), it is possible that it contains a virus, Rad, paragraphs 13-16nad 30.

13. **Claims 38, and 39** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum, Brown, and Schnurrer, as applied to claim 32 above, and further in view of Corthell (6,192,477 B1), Horwitt, and Rad.

In reference to 38 and 39, Kellum system also converts the e-mail message from an executable format to a non-executable format, claim 1 lines 14-18. This would deactivate the executable code.

Kellum, Brown, and Schnurrer do not disclose server for determining whether the executable code has been altered, using an check-summing algorithmic technique.

Corthell discloses a system that uses the checksum algorithm to determine whether a file has been altered, column 8 lines 7-16.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to determine whether the executable code has been altered, using a checksum algorithm, as shown by Corthell. Then deactivate the executable code if it has been altered, using the method disclosed by Kellum. One of ordinary skill in the art would have been motivated to do this because checksum is a common algorithm of checking the corruption of files, Horwitt, abstract. If the file has been corrupted (altered), it is possible that it contains a virus, Rad, paragraphs 13-16 and 30.

14. **Claims 14, 29, and 40** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum, Microsoft Computer dictionary, Ji, Jury, Corthell (6,192,477 B1), Horwitt, and Rad. as applied to claims 12, 27, and 38 respectively above, and further in view of Helbig Sr. et al (6,311,273 B1).

Kellum, Microsoft Computer dictionary, Ji, Jury, Corthell (6,192,477 B1), Horwitt, and Rad do not disclose a method that utilizes a hashing function.

Helbig discloses the use of a hashing algorithm to determine if control software has been altered, column 1 lines 57-60.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to determine whether the executable code has been altered, using a hashing algorithm, as shown by Helbig. Then deactivate the executable code if it has been altered, using the method disclosed by Kellum. One of ordinary skill in the art would have been motivated to do this because a hashing function is a secure method of determining that code has not changed and thus that the trusted code has not been altered, column 1 lines 65-68.

15. **Claims 15, 30, and 41** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum and the Microsoft Computer dictionary as applied to claims 1, 16, and 31 above, and further in view of Field et al (6, 253, 324).

Kellum does not disclose a method where a copy is make of the executable code, executing the first copy and not the second copy and comparing the effect of the executable code.

Field discloses a system where executable code is stored in an image file and the same code is copied and then executed in and executable image. Then a comparison is made of the non-writeable sections of the executable image and that of the verified image file. If the images match then the client is verified, column 2 lines 30-45.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to make a copy of the executable code in the IDS and run one copy and not the other in order to compare the result of running the code, as disclosed by Field. Then deactivate the executable code if it has been altered. One of ordinary skill in the art would have been motivated to do this because running one copy of the code and not the other a way to detect attacking programs that modify memory images of legitimate programs in order to alter its execution, column 2, lines 17-27.

Response to Arguments

16. Applicant's arguments with respect to claim 1-411 have been considered but are moot in view of the new ground(s) of rejection.

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100